ZIW/AF
$

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No.
DE920000127US1

In Re Application Of: **Hamann et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/016,907	**12/14/2001**	**Reagan, James A.**	**45541**	**3621**	**9596**

Invention: **BACK-UP AND USAGE OF SECURE COPIES OF SMART CARD DATA OBJECTS**

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on **February 17, 2005**

The fee for filing this Appeal Brief is: **$500.00**

☐ A check in the amount of the fee is enclosed.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **09-0461 (IBM)**

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **June 23, 2005**

**Ronald A. D'Alessandro
Reg. No. 42456
Hoffman, Warnick & D'Alessandro LLC
Three E-Comm Square
Albany, New York 12207
(518) 449-0044**

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

June 23, 2005.
(Date)

Ashley Bilby
Signature of Person Mailing Correspondence

Ashley Bilby
Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Hamann *et al.*	**Conf. No.:**	9596
Serial No.:	10/016,907	**Art Unit:**	3621
Filing Date:	12/14/2001	**Examiner:**	Reagan, James A.
Title:	BACK-UP AND USAGE OF SECURE COPIES OF SMART CARD DATA OBJECTS	**Docket No.:**	DE920000127US1 (IBMR-0102)

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDED BRIEF OF APPELLANTS

This is an appeal from the Final Rejection dated November 17, 2004, rejecting claims 1-12. This Brief is accompanied by the requisite fee set forth in 37 C.F.R. 1.17 (c).

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case included claims 1-12. No claims have been added. Claims 1-12 remain pending. Claims 1-12 stand rejected and form the basis of this appeal.

STATUS OF AMENDMENTS

Appellant filed an After-Final Response on January 18, 2004. An Advisory Action stating that the Response was considered but did not place the application in condition for allowance was mailed on February 10, 2005.

SUMMARY OF THE INVENTION

The present invention discloses a system and method for back-up and usage of secure copies of smart card data objects, providing a virtual smart card (VSC) having the same defined logical file structure and the same content of data objects as its assigned real smart card, a virtual smart control program handling the creation as well as the read/write process of the VSC, a communication component allowing communication between the virtual smart card and its assigned real smart card, and preferably a smart card manager graphical user interface component allowing different actions with respect to data objects to be securely copied on the virtual or real smart card via the communication component.

The VSC is a software implemented version of a real smart card providing the equivalent functionality of a real smart card. The VSC is created and used by a VSC control program handling the creation, the security and the read/write process of the VSC.

The present invention also provides a VSC having a logical file structure comprising a public area, a private area, a secure key area, a password area, and a unique identifier area. The data objects contained in the public area have no access restrictions, while data objects placed into the private area are encrypted and can be accessed by using a password, and data objects placed into the secure key area are encrypted and only accessible by the VSC control program. Each VSC may be addressed by a unique identifier (ID).

All data objects can be stored and retrieved on/from the virtual smart card's public and private area via the virtual smart card control program using the communication component.

The smart card manager graphical user interface component allows different tasks to create and to use VSCs and handles different tasks required for real smart cards and VSCs to handle data objects, e.g., importing/exporting, copying/pasting data objects.

Claim 1 claims a system for back-up of data objects stored on a real smart card comprising: a virtual smart card control component for handling creating of a virtual smart card and for providing the security and the read/write process for the virtual smart card (see e.g., page 8, line 15 through page 9, line 10; FIG. 2, #8); a smart card manager component for providing a menu controlled graphical user interface allowing user actions for initiating creation of a VSC and back-up of data objects being stored in said real smart into said corresponding area of said virtual smart card (see e.g., page 9, lines16-26; FIG. 2, #18); and a communication component for transferring said data objects to be backed-up from said real smart card to said virtual smart card by using functionality of said virtual smart card control component (see e.g., page 9, lines 11-15, page10, lines 1-10; FIG. 2, #12, 14, 20, 22, 26 and 28).

Claim 2 claims a system for secure copy of data objects being stored in a virtual smart card into a real smart card comprising: a storage media for providing a virtual smart card having data objects to be securely copied into the assigned area of a real smart card (See e.g., page 8, line 15 through page 9, line 10, FIG. 1, #2, 4, 6); a virtual smart card control component for handling creating of a virtual smart card and for providing the security and the read/write process for the virtual smart card (VSC) (see e.g., page 8, line 15 through page 9, line 10; FIG. 2, #8); a communication component for providing access to a real smart card via access to a smart card driver assigned to the smart card reader and a card agent for providing smart card specific commands for writing said data objects to be securely copied from an intermediate buffer of said virtual smart card into said assigned area of said real smart card (see e.g., page 9, lines 11-15, page10, lines 1-10; FIG. 2, #12, 14, 20, 22, 26 and 28); and a smart card manager component providing a menu controlled graphical user interface allowing to initiate user actions for creation of a VSC and secure copy of data objects being stored in said virtual smart card into said corresponding area of said real smart card (see e.g., page 9, lines16-26; FIG. 2, #18).

Claim 5 claims a method to back-up of data objects being stored on a real smart card, characterized by the steps of: opening and displaying data objects of the real smart card to be backed-up via a smart card manager graphical user interface (see e.g., page 11, lines 6-22; FIGS. 3A-3C); selecting data objects to be backed-up via said smart card manager graphical user interface (see e.g., page 11, lines 23-24; FIG. 3E); automatically creating a virtual smart card (VSC) by a smart card control component via said smart card manager graphical user interface, wherein said created virtual smart card having a defined logical file structure being identical with a logical file structure of said real smart card in use (see e.g., page 12, lines 9-11; FIG. 3H); opening a data object area of said created virtual smart card for placing said data objects to be backed-up via said smart card manager graphical user interface (see e.g., page 12, line 22 through page 13, line 4; FIG. 3M); copying data objects to be selected into said area of said created virtual smart card via said smart card manager graphical user interface (see e.g., page 13, lines 3-9; FIGS. 3N-3P); and storing said virtual smart card on a secure permanent storage media (see e.g., page 13, lines 9-14; FIG. 3P).

Claim 12 claims a computer program product stored on a computer usable medium comprising computer readable program means for causing a computer to perform the following method: opening and displaying data objects of the real smart card to be backed-up via a smart card manager graphical user interface (see e.g., page 11, lines 6-22; FIGS. 3A-3C); selecting data objects to be backed-up via said smart card manager graphical user interface (see e.g., page 11, lines 23-24; FIG. 3E); automatically creating a virtual smart card (VSC) by a smart card control component via said smart card manager graphical user interface, wherein said created virtual smart card having a defined logical file structure being identical with a logical file structure of said real smart card in use (see e.g., page 12, lines 9-11; FIG. 3H); opening a data object area of said created virtual smart card for placing said data objects to be backed-up via said smart card manager graphical user interface (see e.g., page 12, line 22 through page 13, line 4; FIG. 3M); copying data objects to be selected into said area of said created virtual smart card via said smart card manager graphical user interface (see e.g., page 13, lines 3-9; FIGS. 3N-3P); and storing said virtual smart card on a secure permanent storage media (see e.g., page 13, lines 9-14; FIG. 3P).

ISSUES

1. Whether claims 1-12 are unpatentable under 35 U.S.C. §103(a) over Benson (EP Patent No. 0 936 530 A1), hereafter "Benson" in view of Mooney *et al.* (U.S. Patent No. 6,351,813 B1), hereafter "Mooney".

GROUPING OF CLAIMS

Claims 1-12 stand or fall together.

ARGUMENT

Appellant submits that claims 1-12 are allowable and respectfully requests reversal of the Final rejection. Specifically, claims 1-12 stand rejected under 35 U.S.C. §103(a) over Benson in view of Mooney.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Appellants respectfully submit that the Benson and Mooney references, taken alone or in combination, fail to meet each of the three basic criteria required to establish a *prima facie* case of obviousness. As such, the rejection under 35 U.S.C. §103(a) is defective.

In the above referenced Final Office Action, the Examiner alleges that there is motivation to combine the references because Mooney's alleged techniques of backing up smart cards using a Graphical User Interface protects the smart card owner and issuer from unauthorized use of lost or stolen smart cards. Final Office Action, page 5. The Office's argument is flawed. In particular, as admitted by the Office, Benson does not specifically teach the use of a GUI to facilitate the transfer of files. In fact, one of the express goals of Benson is to eliminate the problem with smart card technology caused by "...its inherent expense and logistic overhead," due to the required purchase of a physical smart card and a physical smart card reader. Col. 3, par. 0009. In sharp contrast, the access control/crypto system of Mooney requires a physical smart card reader and a smart card. Abstract, Fig. 1. As such, combining Mooney with Benson would destroy the intended function of Benson by requiring the acquisition of the physical smart card and reader of Mooney with "...its inherent expense and logistic overhead." Thus, there is no suggestion or motivation to combine the references, and accordingly, the Office has failed to prove a *prima facie* case of obviousness.

In the above referenced Final Office Action, the Examiner further alleges that Benson teaches or suggests a virtual smart card control component for handling the creation of a virtual smart card. In support of this conclusion, the Office instead cites passages in Benson that introduce the concept of a Virtual Smart Card; disclose a Virtual Smart Card reader, which is an emulator that emulates a physical smart card reader; and gives examples of protected information stored by the Virtual Smart Card. Pars. 0011, 0024 and 0025. However, nowhere in the cited passages or elsewhere in Benson is it disclosed how the Virtual Smart Card is created. The Office attempts to cure this deficiency with the unsubstantiated factual assertion that "creation of a VSC is inherent" and a citation from Benson that the Virtual Smart Card is in an idle state at the time of its creation. However, a virtual smart card control component for handling creating of a virtual smart card is not obvious to one skilled in the art, and nowhere in Benson is this feature taught or suggested. In contrast, the claimed invention includes "...a virtual smart card control component for handling the creation of a virtual smart card." Claim 1. As such, the creation of the virtual smart card as included in the claimed invention is not undefined as in Benson, but instead a virtual smart card control component is included for handling creating of a virtual smart card. This feature is not taught in Benson and is not obvious to one skilled in the art.

In the above referenced Final Office Action, the Examiner still further alleges that the cited references teach or suggest a smart card manager component for providing a menu controlled graphical user interface allowing user actions for initiating creation of a VSC and back-up of data objects being stored in said real smart into said corresponding area of said virtual smart card or secure copy of data objects being stored in the virtual smart card into the corresponding area of said real smart card. Instead, the passage of Benson cited by the Office in support of its conclusion teaches a smart card resource manager, which provides communications between the smart card service provider and the Reader Helper Driver. Col. 6, paragraph 23. However, neither in the cited passage nor anywhere else does Benson teach or suggest that its Smart Card Resource Manager is used in the creation of the Virtual Smart Card. Furthermore, Benson does not teach that its Smart Card Resource Manager is used for either back-up of data objects being stored in a real smart card into a corresponding area of the virtual smart card or secure copy of data objects being stored in the Virtual Smart Card into a corresponding area of a real smart card. The Office also cites Mooney, which has Window Interface Diagrams and a Smart Card Access Module, and which provides a means to back up smart cards onto disk media in a secure manner. Col. 4, lines 60-65; col. 13, lines 10-20. However, the Window Interface Diagrams cited by the Office in FIGS. 4-7 of Mooney are used only to encrypt a data file on a computer system using a Smart Card. Col. 4, lines 61-65. Mooney does not teach that its Window Interface Diagrams are used in conjunction with the Smart Card Access Module, nor does Mooney teach that its Window Interface Diagrams are used to create or in any way transfer data from the smart card. The claimed invention, in contrast, includes "...a smart card manager component for providing a menu controlled graphical user interface allowing user actions for initiating creation of a VSC and back-up of data objects being stored in said real smart card into said corresponding area of said virtual smart card." Claim 1. As such, the menu controlled graphical user interface in the current invention is not merely used to encrypt a source file as are the Window Interface Diagrams of Mooney, but rather allows user actions for initiating creation of a virtual smart card and back-up of data objects being stored in a real smart card into a corresponding area of the virtual smart card. Furthermore, whereas the Benson smart card resource manager only provides communications between two elements of the Virtual Smart Card, the smart card manager component as included in the claimed invention includes a menu controlled graphical user interface allowing user actions for initiating creation of a virtual smart card and back-up of data objects being stored in a real smart card into a corresponding area of the virtual smart card. For the above reasons, the combination of the Benson smart card resource manager and the Window Interface Diagrams for encrypting a file of Mooney do not teach or suggest the smart card manager component including a menu controlled graphical user interface allowing user actions for initiating creation of a virtual smart card as in the claimed invention.

In the above referenced Final Office Action, the Examiner yet still further alleges that the cited references teach or suggest transferring said data objects to be backed-up from said real smart card to said virtual smart card. As stated above, Mooney teaches a Smart Card Access Module that provides a means to back up smart cards but does not teach that virtual smart cards are created as a result. Col. 13, lines 10-20. Conversely, Benson teaches a type of Virtual Smart Card but does not teach that it is created as a back up of a real smart card. Par. 0011-0012 and 0024. Nowhere do the combined references teach transferring data objects to be backed up from a real smart card to a virtual smart card. In contrast, the claimed invention includes "...transferring said data objects to be backed-up from said real smart card to said virtual smart card." Claim 1. As such, the data objects to be backed-up from the real smart card are transferred to the virtual smart card.

In the above referenced Final Office Action, the Examiner yet still further alleges that the cited references teach or suggest writing said data objects to be securely copied from an intermediate buffer of said virtual smart card into said assigned area of said real smart card. As stated above, the passages in Benson cited by the Office introduce the concept of a Virtual Smart Card; disclose a Virtual Smart Card reader, which is an emulator that emulates a physical smart card reader; and give examples of protected information stored by the Virtual Smart Card. Pars. 0011, 0024 and 0025. However, nowhere do the cited passages disclose restoring information to a real smart card that previously has been backed up from a real smart card. The Office attempts to cure this deficiency by citing the Mooney Smart Card Access Module that provides a means to back up smart cards. Col. 13, lines 10-20. However, as stated above, this feature of Mooney does not disclose a virtual smart card. Furthermore, Mooney does not disclose restoring the information to the real smart card. In contrast, the claimed invention includes "...writing said data objects to be securely copied from an intermediate buffer of said virtual smart card into said assigned area of said real smart card." Claim 2. Thus, in contrast to Benson, which simply has a Virtual Smart Card, a Virtual Smart Card reader and protected information stored by the Virtual Smart Card, the data objects as included in the present invention are written from an intermediate buffer of the virtual smart card into an assigned area of a real smart card. In addition, the data objects as included in the claimed invention, rather than being backed up onto disk media as in Benson are securely copied into the real smart card. For the above stated reasons, writing the data objects as included in the claimed invention is not taught or suggested by the features disclosed in the combined references.

In summary, Appellants submit that claims 1-12 are allowable because Benson and Mooney, taken alone or in combination, fail to meet each of the three basic criteria required to establish a *prima facie* case of obviousness.

Respectfully submitted,

Ronald A. D'Alessandro
Reg. No.: 42,456

Date: 6/23/05
Hoffman, Warnick & D'Alessandro LLC
Three E-Comm Square
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

APPENDIX

Claim Listing:

1. System for back-up of data objects stored on a real smart card comprising:

a virtual smart card control component for handling creating of a virtual smart card and for providing the security and the read/write process for the virtual smart card;

a smart card manager component for providing a menu controlled graphical user interface allowing user actions for initiating creation of a VSC and back-up of data objects being stored in said real smart into said corresponding area of said virtual smart card; and

a communication component for transferring said data objects to be backed-up from said real smart card to said virtual smart card by using functionality of said virtual smart card control component.

2. System for secure copy of data objects being stored in a virtual smart card into a real smart card comprising:

a storage media for providing a virtual smart card having data objects to be securely copied into the assigned area of a real smart card;

a virtual smart card control component for handling creating of a virtual smart card and for providing the security and the read/write process for the virtual smart card (VSC);

a communication component for providing access to a real smart card via access to a smart card driver assigned to the smart card reader and a card agent for providing smart card specific commands for writing said data objects to be securely copied from an intermediate buffer of said virtual smart card into said assigned area of said real smart card; and

a smart card manager component providing a menu controlled graphical user interface allowing to initiate user actions for creation of a VSC and secure copy of data objects being stored in said virtual smart card into said corresponding area of said real smart card.

3. System according to claim 1, wherein said communication component comprising:

a smart card API component providing an interface to said smart card manger component, an interface to said virtual control component, and an interface to a smart card & SC Reader Handler component providing an interface to all available smart card reader driver(s), wherein said smart card & SC Reader Handler has an interface to a smart card agency component providing an interface to all available smart card agent(s) providing smart card specific commands.

4. System according to claim 1, wherein said smart card API, said smart card manager component and said virtual smart card control component form an integral component.

5. A method to back-up of data objects being stored on a real smart card, characterized by the steps of:

opening and displaying data objects of the real smart card to be backed-up via a smart card manager graphical user interface;

selecting data objects to be backed-up via said smart card manager graphical user interface;

automatically creating a virtual smart card (VSC) by a smart card control component via said smart card manager graphical user interface, wherein said created virtual smart card having a defined logical file structure being identical with a logical file structure of said real smart card in use;

opening a data object area of said created virtual smart card for placing said data objects to be backed-up via said smart card manager graphical user interface;

copying data objects to be selected into said area of said created virtual smart card via said smart card manager graphical user interface; and

storing said virtual smart card on a secure permanent storage media.

6. Method according to claim 5, wherein said step for automatically creating of said virtual smart card comprises the following steps:

automatically creating a defined file structure having defined areas for placing data objects by a virtual smart card control program;

automatically assigning a password and an unique identifier to said defined file structure created and storing both in the respective area of said defined file structure by said virtual smart card control program; and

electronically storing said defined file structure including said data objects on a storage media virtual smart card.

7. Method according to claim 6, wherein said defined file structure of said virtual smart card comprising:

a public area in which public data objects having no access conditions are placed;

a private area in which private data objects being encrypted are placed;

a secret key area in which key data objects being encrypted are placed;

a password area in which a password being encrypted is placed; and

an unique identifier area in which an unique identifier for identifying the VSC is placed.

8. Method according to claim 7, wherein said defined file structure of said virtual smart card is a dedicated file structure containing elementary files for defining the areas in which said data objects are to be placed.

9. Method according to claim 7, wherein user actions via said menu controlled graphical user interface with respect to the private areas of said virtual smart card require the input of a password.

10. Method according to claim 5, wherein said opening, copying, and storing steps are accomplished using a respective functionality provided by the virtual smart card control program.

11. Method according to claim 5, wherein said virtual smart card is created on a server system and is provided to a client system via a secure channel.

12. A computer program product stored on a computer usable medium comprising computer readable program means for causing a computer to perform the following method:

opening and displaying data objects of the real smart card to be backed-up via a smart card manager graphical user interface;

selecting data objects to be backed-up via said smart card manager graphical user interface;

automatically creating a virtual smart card (VSC) by a smart card control component via said smart card manager graphical user interface, wherein said created virtual smart card having a defined logical file structure being identical with a logical file structure of said real smart card in use;

opening a data object area of said created virtual smart card for placing said data objects to be backed-up via said smart card manager graphical user interface;

copying data objects to be selected into said area of said created virtual smart card via said smart card manager graphical user interface; and

storing said virtual smart card on a secure permanent storage media.